Information Security Policies

System Configuration Management Policy

Policy #	IS-22	Effective Date	03/01/2017	Email	policy@buildfire.com
Version	1.0	Contact	Daniel Hindi	Phone	(949) 899-8204

Table of Contents

PURPOSE

This policy defines the requirements for managing defaults configurations and changes to Buildfire production application, computer, and communications systems.

SCOPE

This policy applies to all Buildfire production information systems. This policy applies to all employees and third-parties responsible for managing Buildfire systems.

POLICY

System Configuration Controls

Baseline Standards – All information systems placed into production must conform to minimum security configurations standards defined by the Information Security Department.

Default Passwords - All vendor-supplied default passwords must be changed before any computer or communications system is used for Buildfire business.

User ID Review - Before any production multi-user computer operating system is installed at Buildfire, all privileged user IDs that are not assigned to a specific employee or partner must be renamed or disabled.

Unnecessary Software - Software features that could be used to compromise security, and that are clearly unnecessary in the Buildfire computing environment, must be disabled at the time when software is installed on multi-user systems.

Unnecessary Functionality - All unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers, must be removed from the Buildfire computer and communication infrastructure.

System Administration Remote Management

Remote Access Encryption – All non-local access to Buildfire systems must be encrypted using methods approved by the Information Security Department. All web-based access must use technologies such as SSH, VPN, or SSL/TLS for web-based management and other non-console administrative access.

Patches and Updates

Security Patch Installation Timing - All critical new security patches must be installed on Buildfire computer and communications systems within one month or receipt.

Non-Emergency Patches Installation - Management in charge of every production information system at Buildfire must establish a time period for the installation of non-emergency patches, fixes, and upgrades to software. The maximum time for non-emergency patch installation is one year.

Patch Exception Process - If a patch or fix is not installed due to application conflicts or other incompatibilities, the involved Systems Administrator must promptly document the reason and forward the documentation to the Information Security Department. These unpatched or unfixed vulnerabilities must be addressed and resolved to the satisfaction of the Information Security Department during the next information security review.

Validating Third Party Patches - Systems Administrators are authorized to patch software only if the software is downloaded, or otherwise received, from a trusted and recognized source approved by the Information Security Department. All patch software which comes with a digital signature must have its digital signature positively verified prior to being installed.

Systems Administrators Install/Update Server Software - Only authorized Systems Administrators are permitted to install and/or update software on Buildfire servers

Vulnerability Management

Vulnerability Identification Software – All systems directly-connected to the Internet that store or process sensitive data must be subjected to an automated risk analysis performed via vulnerability identification software at least once a month.

Vulnerability Scan Reviews – The results of all vulnerability assessments of production computer operating systems must be reviewed by technical personnel. All high-risk vulnerabilities must be addressed.

Change Detection Software

System Integrity Checking Software - All Buildfire servers must run, at the very least on a weekly basis, integrity checking software that detects changes in configuration files, system software files, application software files, and other system resources.

Event Monitoring

Security Event Monitoring (SEM) – Buildfire must employ security event monitoring software to facilitate the collection, storage and analysis of system audit logs

VIOLATIONS

Any violation of this policy may result in disciplinary action, up to and including termination of employment. Buildfire reserves the right to notify the appropriate law enforcement authorities of any unlawful activity and to cooperate in any investigation of such activity. Buildfire does not consider conduct in violation of this policy to be within an employee's or partner's course and scope of employment, or the direct consequence of the discharge of the employee's or partner's duties. Accordingly, to the extent permitted by law, Buildfire reserves the right not to defend or pay any damages awarded against employees or partners that result from violation of this policy.

DEFINITIONS

Confidential Information (Sensitive Information) – Any Buildfire information that is not publicly known and includes tangible and intangible information in all forms, such as information that is observed or orally delivered, or is in electronic form, or is written or in other tangible form. Confidential Information may include, but is not limited to, source code, product designs and plans, beta and benchmarking results, patent applications, production methods, product roadmaps, customer lists and information, prospect lists and information, promotional plans, competitive information, names, salaries, skills, positions, pre-public financial results, product costs, and pricing, and employee information and lists including organizational charts. Confidential Information also includes any confidential information received by Buildfire from a third party under a non-disclosure agreement.

Information Asset – Any Buildfire data in any form, and the equipment used to manage, process, or store Buildfire data, that is used in the course of executing business. This includes, but is not limited to, corporate, customer, and partner data.

Production Application – Production Applications are those applications created and maintained by Buildfire for their customers. These do not include third-party application such as Office 365.

System Baseline - The baseline configuration provides information about the components of an information system (e.g., the standard software load for a workstation, server, network component, or mobile device including operating system/installed applications with current version numbers and patch information), network topology, and the logical placement of the component within the system architecture.

Custodian - Guardian or caretaker of data, the agent charged with implementing the controls specified by the owner. The custodian is responsible for the processing and storage of information.

Third Party – Any non-employee of Buildfire who is contractually bound to provide some form of service to Buildfire.

User - Any Buildfire employee or partner who has been authorized to access any Buildfire electronic information resource.

REFERENCES

CPL: 11.3 Systems Management
ISO/IEC 27002 - 14.2 Security in development and support processes

APPROVAL AND REVISION HISTORY

Version	Description	Revision Date	Approved By:	Title
1.0	Initial Version	03/01/2017	Daniel Hindi	CTO